UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Richmond Division

Leticia Carter, Steven Tellander, Joshua Zipperman, Joalla Rivera, Salvador Gomez Corona, Donald Osborn, Julia and John Gordon, and Gina Valvo, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

Capital One Financial Corporation, Capital One, N.A., and Capital One Bank,

Defendants.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Civil Action No. 3:19cv557

For this Class Action Complaint, Plaintiffs Leticia Carter ("Carter"), Steven Tellander ("Tellander"), Joshua Zipperman ("Zipperman"), Joalla Rivera ("Rivera"), Salvador Gomez Corona ("Corona"), Donald Osborn ("Osborn"), Julia and John Gordon ("Gordon"), and Gina Valvo ("Valvo") (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following against Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (collectively, "Capital One," or "Defendants"), based on personal knowledge as to themselves and their own acts and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through their undersigned counsel:

SUMMARY OF THE CASE

1. This case involves a massive data breach, which Defendants knew about for months before announcing it on July 30, 2019 ("the Data Breach" or "Capital One Data Breach"). The breach involves the improper exposure of the personal information of over 100 million individuals in the United States and Canada, because of Capital One's failure to protect that information – including financial information (e.g., bank account numbers, fragments of transaction history, self-reported income, and credit scores), and/or personal information (e.g., Social Security Numbers, names, addresses, phone numbers, email addresses, and dates of birth).

2. Capital One maintains a privacy policy that makes specific representations to its users regarding its affirmative duty to protect users' personal information, specifically providing that users are in control of who has access to their personal information.[1]

3. As part of the application process and as a result of maintaining a Capital One account and/or credit card, Plaintiffs and Class members were required to provide significate amounts of Personally Identifiable Information ("PII"), including their names, birthdates, home and work addresses, email addresses, consumer credit scores, bank account numbers, telephone numbers, and self-reported income/employment history. They were also required to provide significant amounts of sensitive financial information.

[1] https://www.capitalone.com/bank/privacy/ (Last visited July 31, 2019)

4. The PII and sensitive financial information of Plaintiffs and Class members was supposed to be protected and shared only with expressed permissions and limitations, yet in March 2019, a malicious third-party hacked into Capital One's system, and as a result the PII and sensitive financial information of over 100 million Capital One customers was compromised and stolen.

5. Although Capital One was aware of the breach as early as April 2019, instead of choosing to be transparent about the Data Breach, Capital One waited nearly four months to disclose the Data Breach to the public.

6. Defendants' failure to maintain adequate security measures to protect the PII and sensitive financial information of its customers, was the direct and proximate cause of the injuries to Plaintiffs and Class members, as alleged herein.

7. Plaintiffs and Class members retain a significant interest in ensuring that their PII and sensitive financial data, which are still in Defendants' possession, are protected from further breaches.

8. This Class Action Complaint is filed on behalf of all persons in the United States, described more fully *infra*, whose PII or other personal information was compromised in the Data Breaches.

JURISDICTION AND VENUE

9. This court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state from Defendants and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District and Division. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District and Division.

PARTIES

Plaintiffs

11. Plaintiff Leticia Carter is a resident and citizen of Colorado. Carter first applied for a Capital One credit card in 2017, as well as an automobile loan that same year. Since then, she has used the credit card regularly, including for online payments and auto-payments such that her Capital One card is linked to other online accounts. At all relevant times Carter trusted Defendants with her sensitive personal and financial information. On July 8, 2019, Carter received an email from CreditWise, a credit monitoring service offered by Capital One, stating "Heads up: CreditWise found your personal information somewhere on the dark web." Since learning of the Data Breach and the fact that her personal information existed on the dark web without her consent or permission, she has experienced severe stress and anxiety and spent several hours monitoring her accounts to protect her credit and monitor for fraudulent or suspicious activity. She anticipates spending more time and money in the future doing so.

12. Plaintiff Steven Tellander is a resident and citizen of Colorado. Tellander first applied for a Capital One credit card approximately four years ago, and has used it regularly during that time period. At all relevant times Tellander trusted Defendants with his sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, he has spent several hours monitoring his accounts and trying to protect his credit, and anticipates spending more time and money in the future doing so. He has experienced severe stress and anxiety since discovering he might have been subject to the breach.

13. Plaintiff Joshua Zipperman is a resident and citizen of California. Zipperman first applied for a Capital One credit card, and has been a Capital One customer, since 2001. He has used his Capital One credit card regularly during that time period. At all relevant times, Zipperman trusted Defendants with his sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, he has spent several hours monitoring his accounts and trying to protect his credit and anticipates spending more time and money in the future doing so. He has experienced severe stress and anxiety since discovering he might have been subject to the breach.

14. Plaintiff Joalla Rivera is a resident and citizen of California. Rivera first applied for a Capital One credit card in late-2018 and has used her Capital One credit card regularly during that time period. At all relevant times, Rivera trusted Defendants with her sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, she has spent several hours monitoring her accounts and trying to protect her credit. She anticipates spending more time and money in the future doing so as well. She has experienced severe stress and anxiety since discovering she might have been subject to the breach.

15. Plaintiff Salvador Gomez Corona is a resident and citizen of California. Corona first applied for a Capital One credit card in 2009 and has been a Capital One customer since then. He has used his Capital One credit card regularly during that time period. At all relevant times, Corona trusted Defendants with his sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, he has spent several hours monitoring his accounts and trying to protect his credit. After finding out about the breach, he ordered a copy of his credit report and anticipates spending more time and money in the future as a result of the breach. He has experienced severe stress and anxiety since discovering he might have been subject to the breach.

16. Plaintiff Donald Osborne is a resident and citizen of California. Osborne first applied for a Capital One credit card in 2018 and has been a Capital One customer since then. He has used his Capital One credit Card regularly during that time period. At all relevant times, Osborne trusted Defendants with his sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, he has spent several hours monitoring his accounts and trying to protect his credit and anticipates spending more time and money in the future doing so. He has experienced severe stress and anxiety since discovering he might have been subject to the breach.

17. Plaintiff Julia Gordon is a resident and citizen of California. Ms. Gordon first applied for a Capital One credit card in or around 2016 and has used her Capital One credit card regularly during that time period. At all relevant times, Ms. Gordon trusted Defendants with her sensitive personal and financial information. Since finding out about the Data Breach on July 30,

2019, she has spent several hours monitoring her financial accounts and trying to protect her credit. She anticipates spending more time and money in the future doing so as well. She has experienced severe stress and anxiety since discovering she might have been subject to the breach.

18. Plaintiff John Gordon is a resident and citizen of California. Mr. Gordon first applied for a Capital One credit card in 2014 and has been a Capital One customer since then. He has used his Capital One credit Card regularly during that time period. At all relevant times, Mr. Gordon trusted Defendants with his sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, he has spent several hours monitoring his financial accounts and trying to protect his credit and anticipates spending more time and money in the future doing so. He has experienced severe stress and anxiety since discovering he might have been subject to the breach.

19. Plaintiff Gina Valvo is a resident and citizen of California. Valvo first applied for a Capital One credit card in or around 2009 and has used her Capital One credit card regularly from 2009 through July 2019. At all relevant times, Valvo trusted Defendants with her sensitive personal and financial information. Since finding out about the Data Breach on July 30, 2019, she has spent several hours monitoring her financial accounts and trying to protect her credit. She anticipates spending more time and money in the future doing so as well. She has experienced stress and anxiety since discovering she might have been subject to the breach.

Defendants

20. Defendant Capital One Financial Corporation is incorporated in Delaware and has a principle place of business located at 1680 Capital One Dr., McLean, VA 22102. It offers a broad range of financial services, products, and instruments to consumers, including credit cards. It is among the biggest banks in the United States, with over $370 billion in total assets.

21. Defendant Capital One Bank (USA) is one of two primary subsidiaries of Capital One Financial Corporation. It offers a variety of products to consumers, most notably credit and debit cards.

22. Defendant Capital One, National Association, is the other of Capital One Financial Corporation's two primary subsidiaries. It offers a range of banking and financial products and services to consumers, small businesses, and commercial clients.

23. At all relevant times, Defendants were and are engaged in business in Denver County and throughout the United States of America.

FACTUAL BACKGROUND

A. Defendants Collected and Stored its Clients' Sensitive Personal and Financial Information

24. At all relevant times, Capital One has maintained a Privacy Policy that makes specific representations to Users regarding its protection and exposure of their personal information.

25. The Privacy Policy states that they collect the customers' personal information when they open an account or deposit money, pay their bills or apply for a loan, or use their credit or debit card. It also states that "[w]e also collect your personal information from others, such as credit bureaus, affiliates, or other companies."[2]

26. Capital One represents to Users in its Privacy Policy that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[3]

27. Capital One promised customers that it will keep their Sensitive Information confidential, assuring customers on its credit card applications explicitly that "Capital One uses 256-bit Secure Sockets Layer (SSL) technology. This means that when you are on our website, the data transferred between Capital One and you is encrypted and cannot be viewed by any other party."[4]

28. The Capital One Privacy Policy also states that "[f]ederal law also requires us to

[2] https://www.capitalone.com/bank/privacy/ (Last visited July 31, 2019)
[3] *Id.*
[4] *Id.*

tell you how we collect, share, and protect your personal information."

B. The Data Breach

29. The Data Breach occurred on March 22 and 23, 2019, yet was not publicly disclosed until July 29, 2019, over four months after the PII and sensitive financial information of over 100 million customers and credit card applicants were breached. The hacker could have had access to Capital One systems for over one month, into April 2019.

30. Defendants only discovered the Data Breach after an individual previously unknown to Capital One sent an following email to Capital One providing a link to a file containing the leaked data. The file provided in the link, which was timestamped April 21, 2019, and also contained code for commands used in the intrusion, as well as a list of more than 700 folders of data.

31. On July 29, Capital One finally publicly announced the Data Breach, stating that on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained the personal information of people who had applied for its credit card products, and to Capital One credit card customers. Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million individuals in Canada who had applied for a Capital One credit card product from 2005 through early 2019.[5]

32. Capital One further disclosed that the compromised data included Personal information, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. It also included Customer status data, such as credit scores, credit limits, balances, payment history, and contact information. Furthermore, the compromised data included fragments of transactional data from a total of 23 days during 2016, 2017, and 2018, at least 140,000 Social Security numbers of its credit card customers, and at least 80,000 linked bank account numbers of its secured credit card customers

33. Defendants' security failures demonstrate that they failed to honor their duties and

[5] https://www.prnewswire.com/news-releases/capital-one-announces-data-security-incident-300892738.html (last visited July 31, 2019).

promises by failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks, failing to adequately monitor its system to identify the data breaches and cyber-attacks, and failing to adequately protect Plaintiffs and the Class members' PII and sensitive financial information.

C. PII Is An Increasingly Valuable Commodity

34. PII and sensitive financial information, such as that encompassed in the Capital One Data Breach, is incredibly valuable to companies and to third parties, malicious or otherwise.

35. One study found that an average consumer in the U.S. can make $240 per year monetizing their data for digital advertising.[6] Another study in 2018 found that social media advertising revenue currently amounts to $67.97 billion, and the average revenue per Internet user currently amounts to approximately $22.84 per user.[7] Similarly, a 2016 study found that Google makes approximately $7.00 per monthly active user each quarter, or approximately $28.00 per user each year.[8]

36. Additionally, the types of personal information compromised in the Capital One Data Breach are highly valuable to identity thieves. The full names, birthdates, home and work addresses, email addresses, consumer credit scores, bank account numbers, telephone numbers, self-reported income/employment history, and other valuable PII can all be used to gain access to a variety of existing financial accounts and websites.

37. A 2013 Norton report – based on one of the largest consumer cybercrime studies ever conducted – estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298 dollars.[9]

---

[6] "How Much is Your Data Worth? At Least $240 per Year. Likely Much More," Medium. *Available at* https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa (last visited October 15, 2018).
[7] "Social Media Advertising." Statista. *Available at* https://www.statista.com/outlook/220/100/social-media-advertising/worldwide#market-revenuePerInternetUser (last visited October 15, 2018).
[8] "Facebook Closes the Gap on Google." Ampere Analysis. *Available at https://www.ampereanalysis.com/blog/fd5b6dc9-d76e-40a8-b8f2-e5ed15bc32bb* (last visited October 15, 2018).
[9] 2013 Norton Report. *Available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (last visited October 15, 2018).

38. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud. And indeed Plaintiffs have already spent hours doing so.

39. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII and sensitive financial information they have obtained. Indeed, in order to protect themselves, Class members will need to remain vigilant against unauthorized data use for years and decades to come.

Capital One's Inadequate Data Security Allowed for the Data Breach, Which Was Intentionally Concealed from the Public

40. The Data Breach exposed non-public personal and sensitive financial information – including credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income, credit scores, credit limits, balances, payment history, contact information, and transactional data.[10]

41. Capital One represented that this vulnerability could have potentially affected up to 100 million Capital One clients in the United States that had applied for and/or used Capital One products or services (particularly credit cards) from 2005 through 2019. They also stated that the Social Insurance Numbers of approximately 1 million Canadian credit card customers were compromised in this incident.[11]

42. The Data Breach, like Facebook's Cambridge Analytica scandal, made it possible for third-parties to access private information and sensitive financial information about Capital One clients who never had an opportunity to consent.

[10] https://www.prnewswire.com/news-releases/capital-one-announces-data-security-incident-300892738.html (Last visited July 31, 2019).
[11] *Id.*

43. Although Capital One claimed that "no credit card account numbers or log-in credentials were compromised and over 99 percent of Social Security numbers were not compromised," Capital One also noted that the investigation was still ongoing.[12] Thus, based on Capital One's own admission, the full extent of the damage caused by Capital One's failure to provide adequate controls and protection to Plaintiffs and Class members is yet unknown. Accordingly, the number of impacted individuals, as well as the third-party or parties that may have been able to exploit the vulnerability to access Plaintiff and Class members' PII and sensitive financial information may have been significantly more than what Capital One has yet disclosed.

44. Equally troubling to the widespread and unknown impact of the Data Breach is Capital One's intentional effort, approved by its upper management, to conceal the breach from the public and its victims.

45. Capital One's failure to adequately disclose the vulnerability for months on end has made the potential damage done in the data breach even greater than if Capital One had simply disclosed it when it occurred.

46. The Data Breach has caused significant harm to Plaintiffs and other Class Members by allowing a third-party or parties to access their PII and sensitive financial information without their consent. This harm was exacerbated by Capital One's culture of concealment and opacity regarding its insufficient data protection policies and resulting data breach.

47. Despite this gross lapse in its approach to data security, Capital One still lacks sufficient safeguards and protections for Users' PII and sensitive financial information, and has shown a conscious disregard for any transparency regarding the potential exposure of this personal information. Thus, this personal information remains at risk today and into the future, until Capital One is compelled to secure its User's PII and sensitive financial information.

[12] *Id.*

CLASS ACTION ALLEGATIONS

48. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Classes and Sub-Classes:

> **Nationwide Class**: All persons who applied for and/or obtained Capital One accounts in the United States and whose personal or financial information was accessed, compromised, or obtained from Capital One by any third party or parties without authorization, or in excess of authorization as a result of the Capital One Data Breaches.
>
> **Colorado Sub-Class**: All persons who applied for and/or obtained Capital One accounts in Colorado and whose personal or financial information was accessed, compromised, or obtained from Capital One by any third party or parties without authorization, or in excess of authorization as a result of the Capital One Data Breaches.
>
> **California Sub-Class**: All persons who applied for and/or obtained Capital One accounts in California and whose personal or financial information was accessed, compromised, or obtained from Capital One by any third party or parties without authorization, or in excess of authorization as a result of the Capital One Data Breaches.

49. Excluded from the Classes and Sub-Classes are Defendants and any entities in which Defendants or their subsidiaries or affiliates have a controlling interest, as well as Defendants' officers, agents, and employees. Also excluded from the Class and Sub-Classes are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family. Plaintiffs reserve the right to amend the Class and Sub-Class definitions if discovery and further investigation reveal that any definitions should be expanded or otherwise modified.

50. **Numerosity:** The members of each Class and Sub-Class are so numerous that joinder of all members of every Class and Sub-Class would be impracticable. Plaintiffs reasonably believe that Class and Sub-Class members number hundreds of thousands of people or more in the

aggregate and well over 1,000 in the smallest of the classes. The names and addresses of Class and Sub-Class members are identifiable through documents maintained by Defendants.

51. **Commonality and Predominance**: This action involves common questions of law or fact, which predominate over any questions affecting individual Class and Sub-Class members, including:

a. Whether Defendants represented that Capital One would safeguard Plaintiffs' and Class members' PII and sensitive financial information;

b. Whether Defendants owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their PII and sensitive financial information;

c. Whether Defendants breached a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their PII and sensitive financial information;

d. Whether a third party or parties improperly obtained Plaintiffs' and Class members' PII and sensitive financial information without authorization or in excess of any authorization;

e. Whether Defendants were aware of the third party or parties' collection of Plaintiffs' and Class members' PII and sensitive financial information without authorization or in excess of any authorization;

f. Whether Defendants knew about the Capital One Data Breach before they announced them to the public;

g. Whether Defendants failed to timely notify victims and the public of the Capital One Data Breach;

h. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

i. Whether Defendants' conduct violated the Colorado Security Breach Notification Act, Colo Rev. Stat. 6-1-716, *et seq.*;

j. Whether Defendants' conduct violated § 5 of the FTC Act, 15 U.S.C. § 45, *et seq.*;

k. Whether Plaintiffs and Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

l. Whether Plaintiffs and Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

52. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of the Class and Sub-Classes. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

53. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiffs and Class and Sub-Class members were injured through the substantially uniform misconduct by Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class and Sub-Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class and Sub-Class members arise from the same operative facts and are based on the same legal theories.

54. **Adequacy of Representation**: Plaintiffs are adequate representatives of the Class and Sub-Classes because their interests do not conflict with the interests of the other Class and Sub-Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation; and they will prosecute this action vigorously. Class and Sub-Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

55. **Superiority**: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class and Sub-Class members are relatively small

compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class and Sub-Class members to individually seek redress for Defendants' wrongful conduct. Even if Class and Sub-Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

56. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and Sub-Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class and Sub-Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

57. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class members' PII and sensitive financial information was improperly obtained by third parties;

b. Whether (and when) Defendants knew about any security vulnerabilities that led to the Data Breach before they were announced to victims and the public;

c. Whether Defendants failed to timely notify victims and the public of security vulnerabilities and the Data Breach;

d. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.;*

e. Whether Defendants' representations that Capital One would secure and protect the Personal Information of Plaintiffs and members of the Class and Sub-Class

were facts that reasonable persons could be expected to rely upon when deciding whether to apply for and/or use a Capital One account or credit card;

f. Whether Defendants misrepresented the safety of Capital One's many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and Class and Sub-Class members' Personal Information and sensitive financial information;

g. Whether Defendants concealed crucial information about Capital One's inadequate data security measures from Plaintiffs, the Class, and Sub-Class;

h. Whether Defendants failed to comply with Capital One's own policies and applicable laws, regulations, and industry standards relating to data security;

i. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' Personal Information and sensitive financial information secure and/or prevent the loss or misuse of that information;

j. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and other Class members' PII and sensitive financial information in violation of subdivision (b) and § 5 of the FTC Act;

k. Whether Defendants' conduct violated the Colorado Security Breach Notification Act;

l. Whether Defendants owed a duty to Plaintiffs and Class members to safeguard their Personal Information and sensitive financial information, and to implement adequate data security measures;

m. Whether Defendants breached that duty;

n. Whether such representations were false with regard to storing and safeguarding Plaintiffs' and Class members' PII and sensitive financial information; and

o. Whether such representations were material with regard to storing and safeguarding Plaintiffs' and Class members' PII and sensitive financial information.

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief
Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice (Cal. Bus. & Prof. Code § 17200, *et seq*.)

58. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

59. Capital One's terms of service provides that "This Agreement is governed by and interpreted in accordance with all applicable federal laws and regulations and, as this Agreement applies to each individual account that you may access using the Services, by the state laws and regulations governing such account or the account agreement for such account (to the extent the state laws are not superseded by federal law). Refer to your account agreement to determine in which state your account is located."

60. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

61. Capital One represented that it would not disclose Capital One users' PII and sensitive financial information without consent and/or notice. Capital One further represented that it would utilize sufficient data security protocols and mechanisms to protect Capital One clients' PIIs.

62. Defendants failed to abide by these representations. Defendants did not prevent improper exposure of Plaintiffs' and Class members' PII and sensitive financial information.

63. Defendants stored the PII and sensitive financial information of Plaintiffs and other Class members in electronic and consumer information databases. Defendants falsely represented to Plaintiffs and other Class members that the databases were secure and that their PII and sensitive financial information would remain private. Defendants knew or should have known Capital One did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the other Class members' PII secure and prevented the loss or misuse of their PII.

64. Even without these misrepresentations, Plaintiffs and other Class members were entitled to assume, and did assume Defendants would take appropriate measures to keep their PII and sensitive financial information safe. Defendants did not disclose at any time that Plaintiffs' PII and sensitive financial information was accessible to third party application vendors because Defendants' data security measures were inadequate, and Defendants were the only ones in possession of that material information, which they had a duty to disclose. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of Capital One's many systems and services, and its ability to honor the exposure authorizations established by Plaintiffs and other Class members for their PII and sensitive financial information.

65. Defendants also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and failing to comply with Capital One's own posted privacy policies. If Defendants had complied with these legal requirements, Plaintiffs and other Class members would not have suffered the damages described herein.

66. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), § 5(a) of the FTC Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a result of Capital One failing to comply with its own posted privacy policies).

67. Plaintiffs and other Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In particular, Plaintiffs' and other Class members' PII and sensitive financial information was taken and is now in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that information is of tangible value.

68. As a result of Defendants' unlawful business practices, which are violations of the UCL, Plaintiffs and the Class members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Second Claim for Relief
Violation of California's UCL – Unfair Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq*.)

69. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

70. By reason of the conduct alleged herein, Defendants engaging in unfair "business practices" within the meaning of the UCL.

71. Defendants stored the PII and sensitive financial information of Plaintiffs and other Class members in electronic and consumer information databases. Defendants represented to Plaintiffs and other Class members that the databases were secure and that their PII and sensitive financial information would remain private and be exposed only with expressed authorization. Defendants engaged in unfair acts and business practices by representing that Capital One would require expressed consent and authorization prior to exposure PII to third parties.

72. Even without these misrepresentations, Plaintiffs and other Class members were entitled to, and did, assume Defendants would take appropriate measures to keep their PII and sensitive financial information safe. Defendants did not disclose at any time that Plaintiffs' and other Class members' PII and sensitive financial information was vulnerable to unauthorized exposure because Capital One's data security measures were inadequate, and Defendants were in sole possession of that material information, which they had a duty to disclose.

73. Defendants knew or should have known Capital One did not employ reasonable measures that would have kept Plaintiffs' and other Class members' PII and sensitive financial information secure from unauthorized exposure.

74. Defendants engaged in unfair acts and business practices by representing that Capital One would not expose Plaintiffs' and other Class members' PII and sensitive financial information without authorization, and/or by obtaining that PII and sensitive financial information without authorization. Defendants also violated Capital One's commitment to maintain the confidentiality and security of the PII and sensitive financial information of Plaintiffs and other

Class members, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.

75. Defendants engaged in unfair business practices under the "balancing test" because the harm caused by their actions and omissions, as described in detail *supra*, greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and misrepresentations to consumers about Capital One's data security cannot be said to have had any utility at all.

76. Defendants engaged in unfair business practices under the "tethering test" because their actions and omissions, as described in detail *supra*, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of Personal Information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that Personal Information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendants' acts and omissions, and the injuries caused by them, are thus "comparable to or the same as a violation of the law ..." *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

77. Defendants engaged in unfair business practices under the "FTC test" because the harm caused by their actions and omissions, as described in detail *supra*, is substantial in that it affects millions of Class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, exposure of Class members' PII and sensitive financial information to the dark web, exposure of Class members' PII and sensitive financial information to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact

that Class members' PII and sensitive financial information remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions and omissions violated, *inter alia*, § 5(a) of the FTC Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure Personal Information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of Personal Information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

78. Plaintiffs and other Class members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. In addition, their PII and sensitive financial information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

79. As a result of Defendants' unfair business practices, which are violations of the UCL, Plaintiffs and other Class members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Third Claim for Relief
Violation of California's UCL – Fraudulent/Deceptive Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq.*)

80. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

81. Capital One engaged in fraudulent and deceptive acts and practices with regard to the services it provided to the Class by representing and advertising that (1) it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII and sensitive financial information from unauthorized disclosure, release, data breaches, and theft and that (2) it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PII and sensitive financial information. These representations were likely to deceive members of the public, including Plaintiff and the Class Members, into believing their PII and sensitive financial information was securely stored – when it was not – and that Capital One was complying with relevant law – when it was not.

82. Capital One engaged in fraudulent and deceptive acts and practices with regard to the services provided to the Class by omitting, suppressing, and concealing the material fact that the privacy and security protections for Class Members' PII was woefully inadequate. At the time that Class members were using Capital One's services, Capital One failed to disclose to Class Members that its data security systems failed to meet legal and industry standards for the protection of their PII and sensitive financial information. These representations likely deceived members of the public, including Plaintiffs and the Class, into believing that their PII was securely stored – when it was not – and that Capital One was complying with relevant law and industry standards – when it was not.

83. As a direct and proximate result of Capital One's deceptive practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII and sensitive financial information, and additional losses described above.

84. Capital One knew or should have known that its computer systems and data security practices were inadequately safeguarding Class Members' PII and sensitive financial information, and that the risk of a data breach or theft was very high.

85. Capital One's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

86. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, et. seq., including, but not limited to, restitution to Plaintiffs and the Class of money or property that Capital One may have acquired by means of its fraudulent and deceptive business practices, restitutionary disgorgement of all profits accruing to Capital One because of its fraudulent and deceptive business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Fourth Claim of Relief
Negligence

87. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

88. Defendants owed a duty to Plaintiffs and other Class members to exercise reasonable care in safeguarding and protecting their PII and sensitive financial information and keeping it from being compromised, lost, stolen, misused, and/or exposed to unauthorized parties.

89. Defendants knew that the PII and sensitive financial information of Plaintiffs and other Class members was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the PII and sensitive financial information of Plaintiffs and other Class members was wrongfully exposed, that exposure was not fixed, or they were not told about the exposure in a timely manner.

90. By entrusting Defendants to safeguard their PII, Plaintiffs and other Class members had a special relationship with Defendants. Plaintiffs and other Class members signed

up for Capital One's services and agreed to provide their PII and sensitive financial information with the understanding that Capital One would take appropriate measures to protect it, and would inform them of any breaches or other security concerns that might call for action by Plaintiffs and other Class members. But Defendants did not. Defendants not only knew Capital One's data security was inadequate, they also knew Capital One did not have the tools to detect and document intrusions or exfiltration of PII. Defendants are morally culpable, given its repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs and other Class members of data breaches or security vulnerabilities.

91. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and other Class members' PII and sensitive financial information by failing to adopt, implement, and maintain adequate security measures to safeguard that information and prevent unauthorized exposure of that PII and sensitive financial information.

92. Defendants also breached their duty to timely disclose that Plaintiffs' and other class members' PII and sensitive financial information had been, or was reasonably believed to have been, improperly exposed.

93. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and other Class members, their PII and sensitive financial information would not have been compromised, stolen, and viewed by unauthorized persons.

94. Defendants' negligence was a direct and legal cause of the theft of the PII and sensitive financial information of Plaintiffs and other Class members and all resulting damages.

95. The injury and harm suffered by Plaintiffs and other Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and other class members' PII and sensitive financial information. Defendants knew Capital One's systems and technologies for processing and securing the PII of Plaintiffs and other Class members had numerous security vulnerabilities.

96. As a result of this misconduct by Defendants, the Personal Information of Plaintiffs and other Class members was compromised, placing them at a greater risk of identity

theft and subjecting them to identity theft, and their PII and sensitive financial information was exposed to third parties without their consent.

Fifth Claim for Relief
Invasion of Privacy

97. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

98. The California Constitution expressly provides for a right to privacy. Cal. Const. Art. I, § 1.

99. Capital One's terms of use for all times relevant to this matter provided that Users' PII would not be exposed to third parties without express consent.

100. Absent their express consent, Plaintiffs and other Class members used Capital One accounts and/or credit cards under the impression that PII and sensitive financial information was safeguarded and would not be provided to or stolen by third parties.

101. Plaintiffs and other Class members had an interest in the protection and non-dissemination of the PII and sensitive financial information that Capital One electronically stored, including the right not to have that PII and sensitive financial information stolen and used for profit.

102. Absent the express consent of Capital One clients, Defendants intentionally intruded on Plaintiffs' and other Class members' private life, seclusion, and solitude, protected under the California constitution as well as common law.

103. Defendants' wrongful conduct constitutes breach of the social norms underpinning the constitutionally-protected right to privacy.

104. Defendants' wrongful conduct harmed Plaintiffs and other Class members.

105. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and other Class members have suffered injury and are entitled to appropriate relief, including injunctive relief and damages.

Sixth Claim for Relief
Deceit by Concealment (Cal. Civil Code §§ 1709, 1710)

106. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

107. As alleged above, Defendants knew its data security measures were grossly inadequate by, at the absolute latest, March 2019.

108. In response, Defendants chose to do nothing to protect Plaintiffs and the Class or warn them about the security problems. Instead, Defendants chose to conceal the breach in order to avoid public backlash.

109. Defendants had an obligation to disclose to all class members that their Capital One accounts, PII, and sensitive financial information were potentially compromised by the data breach.

110. Defendants did not do this. Instead, Defendants willfully deceived Plaintiffs and the Class by concealing the true facts concerning its poor data security, which Defendants were obligated to, and had a duty to, disclose.

111. Had Defendants disclosed the true facts about its poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, which Defendants failed to do.

112. Independent of any representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants to provide a service with at least minimally adequate security measures and to disclose facts undermining that reliance.

113. Rather than disclosing to Plaintiffs and the Class that its services were compromised by the breach and that PII and sensitive financial information was improperly exposed, Defendants continued on, concealing information relating to the inadequacy of its security measures.

114. These actions constitute "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

115. As a result of this deceit by Defendants, they are liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

116. As a result of this deceit by Defendants, the PII and sensitive financial information of Plaintiffs and the Class were compromised, and their PII and sensitive financial information was disclosed to third parties without their consent. Plaintiffs and the other Class members also suffered diminution in value of their PII. Plaintiffs and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

117. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was a deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive damages against Defendant under Civil Code § 3294(a).

Seventh Claim for Relief
Breach of Implied Contract

118. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

119. Capital One solicited and invited Plaintiffs and Class Members to use its products and service. Plaintiffs and Class members accepted Capital One's offers and created credit and/or debit accounts requiring the provision of PII and sensitive financial information to Capital One during the period of the data breach.

120. When Plaintiffs and Class Members used Capital One products and services, they provided their PII and sensitive financial information. In so doing, Plaintiffs and Class Members

entered into implied contracts with Capital One pursuant to which Capital One agreed to safeguard and protect such information.

121. Each use of a Capital One service or product made by Plaintiffs and Class Members was made pursuant to the mutually agreed-upon implied contract with Capital One under which Capital One agreed to safeguard and protect Plaintiffs and Class Members' PII and sensitive financial information.

122. Plaintiffs and Class Members would not have provided and entrusted their PII and sensitive financial information to Capital One in the absence of the implied contract between them and Capital One.

123. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Capital One.

124. Capital One breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the PII and sensitive financial information of Plaintiffs and Class.

125. As a direct and proximate result of Capital One's breaches of the implied contracts between Capital One and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

ADDITIONAL CLAIM ON BEHALF OF THE COLORADO SUB-CLASS ONLY

Eighth Claim for Relief
Violation of Colorado Security Breach Notification Act
(Colo. Rev. Stat 6-1-716, et seq.)

126. Colorado Plaintiffs hereby repeat, reallege and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

127. Colorado Plaintiffs bring this cause of action on behalf of themselves and on behalf of the Colorado Sub-Class who are all Colorado residents.

128. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6 1-716(2).

129. Colorado Plaintiffs and Colorado Subclass's PII and sensitive financial

information includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

130. Under Colo. Rev. Stat. § 6-1-713.5, Defendants "maintains, owns, or licenses personal identifying information of an individual residing in [Colorado]," and thus is required to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

131. Defendants were required to accurately notify Colorado Plaintiffs and the Colorado Subclass when it became aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

132. Because Defendants were aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev Stat. § 6-1-716(2).

133. By failing to disclose the Data Breach for nearly five months, Defendants utterly failed to uphold this obligation.

134. As a direct and proximate result of Defendants' violations of Colo. Rev. Stat. § 6-1-716(2), Colorado Plaintiffs and Colorado Subclass members suffered damages, as described above.

135. Colorado Plaintiffs and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

ADDITIONAL CLAIM ON BEHALF OF THE CALIFORNIA SUB-CLASS ONLY

Ninth Claim for Relief
Violation of California Customer Records Act
(Cal. Civ. Code § 1798.80, *et seq*.)

136. California Plaintiffs hereby repeat, reallege and incorporate by reference each and every allegation contained above as though the same were fully set forth herein.

137. California Plaintiffs bring this cause of action on behalf of themselves and on behalf of the California Sub-Class who are all California residents.

138. The California Legislature enacted Civil Code § 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

139. Defendants are a "business" as defined by Cal. Civ. Code § 1798.80(a).

140. California Plaintiffs and California Sub-Class Members are "individual[s]" as defined by Cal. Civ. Code § 1798.80(d).

141. The personal information taken in the data breach was "personal information" as defined by Cal. Civ. Code § 1798.80(e) and 1798.81.5(d), which includes:

> information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information." "

142. The breach of the incredibly sensitive and confidential PII of 100 million former, current, and prospective Capital One customers was a "breach of the security system" of Defendants as defined by Cal. Civ. Code § 1798.82(g).

143. By failing to implement reasonable security measures which would appropriately secure the personal information of Plaintiffs and Class Members, Defendants violated Cal. Civil Code § 1798.81.5.

144. In addition, by failing to immediately notify all affected Class Members that their personal information had been acquired or may have been acquired by unauthorized persons in the data breach, Defendants violated Cal. Civil Code § 1798.82. Defendants' failure to immediately notify Plaintiffs and Class Members of the breach caused Class Members to suffer damages because they have lost the opportunity to immediately:

a) buy identity protection, monitoring, and recovery services;

b) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service;

c) purchase or otherwise obtain credit reports; monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services;

d) place and renew credit fraud alerts on a quarterly basis;

e) routinely monitor public records, loan data, or criminal records;

f) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts;

g) and, take other steps to protect themselves and recover from identity theft and fraud.

145. Because it violated Cal. Civil Code § 1798.81.5 and 1798.82, Defendants "may be enjoined" under Cal. Civil Code § 1798.84(e).

146. Plaintiffs request that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures to protect Class Members' personal information, including, but not limited to, ordering that Defendants:

a) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

b) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices;

c) audit, test, and train its security personnel regarding any new or modified procedures;

d) purge, delete and destroy, in a secure manner, Class Members' data not

necessary for its business operations;

e) conduct regular database scanning and securing checks consistent with prudent industry practices;

f) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices;

g) receive periodic compliance audits by a third party regarding the security of the computer systems, cloud-based services, and application software Defendants use to store the personal information of current, former, and potential Capital One customers;

h) meaningfully educate its current and former Capital One customers about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and

i) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Class Members.

147. As a result of Defendants' violation of Cal. Civ. Code § 1798.81.5, Plaintiffs and Class Members have incurred and will incur damages, including but not necessarily limited to:

a) the loss of the opportunity to control how their personal information is used;

b) the diminution in the value and/or use of their personal information entrusted to Defendants for the purpose of deriving services from Defendants and with the understanding that Defendants would safeguard their personal information against theft and not allow access and misuse of their personal information by others;

c) the compromise, publication, and/or theft of their personal information;

d) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts;

e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect,

contest and recover from identity data misuse;

f) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;

g) unauthorized use of compromised personal information to open new financial and/or health care or medical accounts;

h) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected;

i) the continued risk to their personal information, which remains in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and

j) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the data breach for the remainder of the lives of the Class Members.

148. Plaintiffs seek all remedies available under Cal. Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class and Sub-Class members, respectfully request that this Court enter an Order:

a. Certifying the United States Class, the California Sub-Class, and the Colorado Sub-Class, and appointing Plaintiffs as Class and Sub-Class Representatives;

b. Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendant from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

d. Awarding Plaintiffs and Class and Sub-Class members actual, compensatory, and consequential damages;

e. Awarding Plaintiffs and Class and Sub-Class members statutory damages and penalties, as allowed by law;

f. Awarding Plaintiffs and Class and Sub-Class members restitution and disgorgement;

g. Requiring Defendant to provide appropriate credit monitoring services to Plaintiffs and the other Class and Sub-Class members;

h. Awarding Plaintiffs and Class and Sub-Class members punitive damages;

i. Awarding Plaintiffs and Class and Sub-Class members pre-judgment and post-judgment interest;

j. Awarding Plaintiffs and Class and Sub-Class members reasonable attorneys' fees costs and expenses, and;

k. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

DATED: August 5, 2019

Respectfully submitted,

/s/

Dale W. Pittman, VSB#15673
THE LAW OFFICE OF DALE W. PITTMAN, P.C.
The Eliza Spotswood House
112-A West Tabb Street
Petersburg, VA 23803-3212
(804) 861-6000
(804) 861-3368 (Fax)
dale@pittmanlawoffice.com

FRANKLIN D. AZAR & ASSOCIATES, P.C.
Ivy T. Ngo (CA SBN 249860)
Joshua E. Moyer (CA SBN 259908)
14426 E. Evans Avenue
Aurora, CO 80014
Telephone: (303) 757-3300
Facsimile: (720) 213-5131
Email: ngoi@fdazar.com
Email: moyerj@fdazar.com

CAPSTONE LAW APC
Mark A. Ozzello (CA SBN 116595)
Tarek H. Zohdy (CA SBN 247775)
Cody R. Padgett (CA SBN 275553)
Trisha K. Monesi (CA SBN 303512)
1875 Century Park East, Suite 1000
Los Angeles, CA 90067
Telephone: (310) 556.6824
Facsimile: (310) 943.0396
Email: Mark.Ozzello@capstonelawyers.com
Email: Tarek.Zohdy@capstonelawyers.com
Email: Cody.Padgett@capstonelawyers.com
Email: Trisha.Monesi@capstonelawyers.com

LOCKRIDGE GRINDAL NAUEN P.L.L.P
Karen H. Riebel
Kate M. Baxter-Kauf
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401-2159
Telephone: (612) 596-4097
Facsimile: (612) 339-0981
Email: khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Counsel for Plaintiffs